

## UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

NEVEAH ROSA YBARRA,

Defendant

Case No. 2:23-mj-00978-duty

<p><b>FILED</b> CLERK, U.S. DISTRICT COURT</p> <p>3/2/2023</p> <p>CENTRAL DISTRICT OF CALIFORNIA</p> <p>BY: <u>DL</u> DEPUTY</p>
--

**CRIMINAL COMPLAINT BY TELEPHONE  
OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of March 1, 2023 in the county of Los Angeles in the Central District of California, the defendant violated:

*Code Section*

18 U.S.C. § 1029(a)(2)

*Offense Description*

Use of unauthorized access devices

This criminal complaint is based on these facts:

*Please see attached affidavit.*

☒ Continued on the attached sheet.

/s/

Complainant's signature

Kyle Krueger, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 3/2/2023

*Rozella A. Oliver*  
Judge's signature

City and state: Los Angeles, California

Hon. Rozella A. Oliver, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT**

I, Kyle Krueger, being duly sworn, declare and state as follows:

**I. PURPOSE OF AFFIDAVIT**

1. This affidavit is made in support of a criminal complaint against Nevaeh Rosa YBARRA ("YBARRA") for a violation of 18 U.S.C. § 1029(a)(2) (use of unauthorized access devices).

2. This affidavit is also made in support of an application for a warrant to search the following digital device in the custody of the United States Secret Service ("USSS"), in Los Angeles, California, as described in Attachment A-1: Samsung Galaxy A14 mobile device with IMEI 350545463176826 (the "SUBJECT DEVICE").

3. This affidavit is also made in support of a search warrant for a 2008 white Toyota Prius, bearing California license plate 8FCB613 and Vehicle Identification Number JTDKB20U583455633 (the "SUBJECT VEHICLE") as described in Attachment A-2.

4. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information), 1029 (Fraud and Related Activity in Connection with Access Devices), 1344 (Bank Fraud), and 1028A (Aggravated Identity Theft) (collectively, the "Subject Offenses"), as described more fully in Attachment B.

5. Attachments A-1, A-2, and B are incorporated herein by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and search warrants, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

## **II. BACKGROUND OF AFFIANT**

7. I am a Special Agent with the USSS and have been so employed since August 2018. Currently, I am assigned to the Los Angeles Field Office Cyber Fraud Task Force. In this capacity, I am responsible for investigating violations of federal and state criminal laws relating to financial-institution fraud, credit-card fraud, bank fraud, cybercrimes, and identity theft. I am a graduate of the Criminal Investigators Training Program conducted at the Federal Law Enforcement Training Center, as well as the USSS Special Agent Training Course in Beltsville, Maryland. I have received continued education related to the investigation and prosecution of financial crimes. In this capacity, I have participated in multiple investigations in connection with fraud and financial crimes.

## **III. SUMMARY OF PROBABLE CAUSE**

8. Between August 2022 and January 2023, the California Department of Social Services ("DSS") has detected more than

\$38.9 million in stolen funds from victim Electronic Benefit Transfer ("EBT") cards. Much of this fraud is from two specific programs known as CalFresh and CalWORKs, which help low-income households pay for housing, food, and other necessary expenses. Many of the fraudulent withdrawals are done at specific ATMs in the Central District of California.

9. For example, between on or about January 1, 2023, and on or about January 5, 2023, more than approximately \$117,000 was withdrawn from ATMs at a single financial institution branch located in Toluca Lake, California in Los Angeles County. The unauthorized withdrawals conducted during these five days and at this single bank branch affected approximately 152 victim EBT cardholders. The dates of these withdrawals coincided with the disbursement by DSS of CalFresh and CalWORKs benefits to EBT cardholders.

10. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding stacks of cards and conducting withdrawals from multiple accounts in quick succession at one ATM.

11. On or about March 1, 2023, at approximately 08:26 a.m. (PST), law enforcement conducted physical surveillance at a US Bank ATM terminal located at 8444 Florence Avenue, Downey, California, which was identified by DSS as one of the top ATM locations for EBT fraud. YBARRA arrived in the SUBJECT VEHICLE and proceeded to the ATM terminal located at the US Bank branch

where law enforcement was conducting surveillance. At the ATM, law enforcement observed, and US Bank confirmed that, YBARRA withdrew cash from the ATM in rapid succession using approximately 7 different access devices, belonging to account holders other than YBARRA. YBARRA was arrested and found to possess 17 access devices belonging to individuals other than YBARRA. The SUBJECT DEVICE was seized from the SUBJECT VEHICLE upon YBARRA's arrest and impounding.

#### **IV. STATEMENT OF PROBABLE CAUSE**

12. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

##### **A. Regulatory Background of CalFresh and CalWORKs Programs**

13. DSS is a government agency that administers several benefit and assistance programs for residents of the state of California. One of the assistance programs administered by DSS is called CalFresh (formerly known as food stamps), which helps low-income households purchase food and household items to meet their nutritional needs. Another assistance program administered by DSS is called CalWORKs, which helps low-income families with children pay for housing, food, and other necessary expenses.

14. Residents of California that meet the criteria established by the CalFresh or CalWORKs programs can apply online for benefits at [www.getcalfresh.org](http://www.getcalfresh.org) and [www.benefitscal.com](http://www.benefitscal.com). Beneficiaries apply for benefits by

submitting their income and number of dependents to determine their benefit eligibility.

15. CalFresh and CalWORKs benefits are issued through Electronic Benefit Transfer cards ("EBT cards"). EBT cards are mailed to an address designated by the account holder and function like traditional debit cards to conduct transactions. For example, you can use an EBT card to make a purchase at a grocery or convenient store by swiping the card at a point-of-sale terminal.

16. The EBT cards issued under CalFresh and CalWORKs are assigned specific Bank Identification Numbers ("BIN"). A BIN refers to the first five digits of the account number on a debit or credit card and can be used to identify the issuer of the card, like DSS, which administers the CalFresh and CalWORKs programs.

17. Benefits received through the program are typically disbursed to EBT cardholders by DSS during the early days of each month. Those benefits are deposited directly from DSS into the account of the EBT cardholder.

18. The EBT cardholders can then conduct cash withdrawals at automated teller machines ("ATMs") using a personal identification number ("PIN") established by the card holder. The EBT cardholder presents the card at an ATM, inserts the card into the ATM card reader, and utilizes a PIN to withdraw the funds previously deposited by DSS intended for beneficiaries of the CalFresh or CalWORKs programs.

**B. Background on EBT Fraud in the Los Angeles Area and Prior State and Federal Operations**

19. Since in or about August 2022, local law enforcement has been working with DSS to investigate a significant increase in unauthorized cash withdrawals utilizing EBT cards. Based on analysis of victim complaints to DSS, victim complaints to local law enforcement, bank records, and surveillance, law enforcement determined that the majority of the unauthorized cash withdrawals were being conducted with cloned cards.

20. A cloned card can be a blank white plastic card or another debit, credit or gift card that contains altered information on the card's magnetic stripe. Based on my training and experience, I know that suspects will often clone cards by taking stolen card information from a victim card's magnetic stripe and re-encode that stolen information onto another card's magnetic stripe. Cloning these cards allows the suspect to use the card and the DSS benefits added on to the account linked to the card for illicit purchases or unauthorized cash withdrawals.

21. On a legitimate debit or credit card, the information coded on the card's magnetic stripe will match the information embossed on the front of the card. This information includes the account number, expiration date, and cardholder's name, among other information. Whereas on a cloned card, the information coded on the magnetic stripe will not match the information embossed on the front of the card. For example, if a suspect re-encodes victim EBT card information onto a pre-existing gift card's magnetic stripe or a blank white plastic

card with a magnetic stripe, the magnetic stripe will be coded with the EBT card information, but the card itself will still bear the information of the gift card or bear no information if it is a blank white plastic card.

22. Based on my training, experience, and participation in this investigation, I know that the victim card data harvested to clone cards is often obtained from what is colloquially referred to as "skimming activity."

23. The term "skimming" is used to describe activity that involves unlawfully obtaining debit and credit card information by using technological devices to surreptitiously record victim accountholder's debit and credit card numbers and personal identification numbers at, for example, ATMs or point-of-sale terminals. For example, individuals conducting ATM "skimming" may install a skimming device into the card reader of the ATM to record the debit or credit card numbers, as well as a camera or keypad overlay on the ATM keypad to record the associated PIN number. Those individuals will then return to the ATM to collect the card number and PIN information stored on the installed device.

24. As described above, suspects then manufacture cloned and fraudulent debit or credit cards that bear the victim accountholder's account information that was obtained from skimming. Once that information is loaded onto another fraudulent card (e.g., a gift card or blank plastic card), members of the scheme then use that fraudulent card to withdraw



cash from the victim accountholder's bank accounts or to make purchases with the victim accountholder's account.

25. In or about September 2022, local law enforcement conducted a surveillance and arrest operation in the Los Angeles, California area. This operation was planned in response to the large number of unauthorized withdrawals occurring at ATMs in the Los Angeles area during a short period of time. Specifically, law enforcement had analyzed fraudulent EBT withdrawal data and noticed a high volume of unauthorized withdrawals on specific dates and times that coincided with the dates when the majority of benefits are disbursed to EBT cardholders.

26. As a result of this operation, local law enforcement established surveillance at select ATMs that were used to conduct a significant volume of EBT fraud. Law enforcement surveilled those ATMs around the dates when benefits had been disbursed, observed suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession, and arrested multiple individuals believed to be making fraudulent withdrawals of EBT benefits. As a result, law enforcement arrested approximately 16 suspects. All of the arrested suspects were later determined to be citizens of countries other than the United States who did not have documentation to be lawfully present in the United States. All of the individuals arrested were released from local custody within hours of their arrest and absconded from any future judicial proceedings.

27. In or about February 2023, in response to a further increase in unauthorized cash withdrawals utilizing EBT cards after the local law enforcement September 2022 operation, federal law enforcement conducted a similar surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed at select high-volume EBT fraud ATMs. Law enforcement arrested three suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession. Two of those defendants came to the ATM together, possessed 35 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that they had made more than \$190,000 in past attempted fraudulent EBT withdrawals from a single bank since October 2022. One additional defendant possessed 269 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that the defendant had made more than \$70,000 in past attempted fraudulent EBT withdrawals from a single bank since January 2023. All three of these defendants were determined to be citizens Romania, who did not have documentation to be lawfully present in the United States. The three arrested defendants were ordered detained pending trial by the Hon. Karen Stevenson and Hon. Margo A. Rocconi. A federal grand jury returned two indictments against the three defendants for bank fraud, in violation of 18 U.S.C. § 1344; aggravated identity theft, in violation of 18 U.S.C. § 1028A; use of unauthorized access devices, in violation 18 U.S.C. §

1029(a)(2); and possession of unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3), in 23-CR-0076-FLA and 23-CR-0077-JFW.

**C. Background of Current Operation to Combat EBT Fraud**

28. Data provided by DSS, based in part upon reported fraud by victims, reported fraud to local law enforcement, bank records, and surveillance indicates that as of in or about January 2023, there has been approximately \$71.3 million in stolen funds from victim EBT cards.

29. For the previous six months, between in or about August 2022 and in or about January 2023, in the Central District of California and elsewhere, more than approximately \$38.9 million has been stolen from victim EBT cards. The majority of these funds were stolen through unauthorized ATM withdrawals.

30. Between on or about January 1, 2023, and on or about January 5, 2023, more than approximately \$7.2 million was stolen from victim EBT cards largely through unauthorized ATM withdrawals. Of the approximately \$7.2 million stolen from victim EBT cards in the beginning of January 2023, more than approximately \$2.9 million was stolen, almost entirely through unauthorized ATM withdrawals, in Los Angeles County alone.

31. For example, between on or about January 1, 2023, and on or about January 5, 2023, more than approximately \$117,000 was withdrawn from ATMs at a single financial institution branch located in Toluca Lake, California in Los Angeles County. The unauthorized withdrawals conducted during these five days and at

this single bank branch affected approximately 152 victim EBT cardholders. The dates of these withdrawals coincided with the disbursement by DSS of EBT benefits, including CalFresh and CalWORKs.

32. Based upon my training and experience conducting access device fraud investigations, I know that suspects committing access device fraud schemes will often target particular BINs when harvesting stolen card information collected from skimming devices. Thus, suspects using skimming may target the BIN associated with DSS, in essence, targeting CalFresh and CalWORKs benefits. Moreover, based upon my training and experience, the sheer volume of unauthorized ATM withdrawals occurring during the early days of the month is further indicative that suspects participating in the fraud scheme at issue are targeting EBT cards because benefits are typically disbursed to EBT cardholders during the early days of each month.

33. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding stacks of cards and conducting withdrawals in quick succession at one ATM. Based upon my training and experience, I know that suspects perpetrating access device fraud schemes will often conduct unauthorized withdrawals using cloned cards in rapid succession at ATMs.

34. Based upon the rapid succession of unauthorized ATM withdrawals being conducted, the fact that the cards being used to conduct the unauthorized cash withdrawals are nearly all cloned EBT cards, and the fact that nearly all of the unauthorized withdrawals are happening during the early days of the month, I believe that suspects participating in the fraud scheme at issue are ostensibly targeting EBT cards.

**D. YBARRA Committed EBT Fraud Using Unauthorized Access Devices and Possessed Unauthorized Access Devices on March 1, 2023**

35. Based upon the large dollar amount being stolen from victim EBT cards, the number of victims impacted, the concentration of unauthorized ATM withdrawals occurring in particular areas, and the large number of unauthorized ATM withdrawals occurring at singular bank locations, law enforcement conducted a surveillance and arrest operation in March 2023.

36. On or about March 1, 2023, law enforcement was conducting physical surveillance at various bank and ATM locations throughout Los Angeles County, including a US Bank ATM terminal located at 8444 Florence Avenue in Downey, California ("US Bank ATM"). Based on DSS fraud data, surveillance was conducted beginning at approximately 4:15 a.m.

37. DSS reported to law enforcement that the CalFresh and CalWORKs benefits had been disbursed into the EBT accounts at approximately 12:00 a.m. on March 1, 2023.

38. USSS agents and Los Angeles District Attorney's Office investigators told me that during this surveillance, law

enforcement observed two unknown individuals, later identified as YBARRA and one minor (hereafter, "minor 1"), arrive in the SUBJECT VEHICLE and approach the US Bank ATM at approximately 08:26 a.m. Law enforcement observed YBARRA in the driver's seat of the SUBJECT VEHICLE with minor 1 as a passenger.

39. USSS agents and Los Angeles District Attorney's Office investigators told me that after YBARRA exited the SUBJECT VEHICLE and approached the US Bank ATM, law enforcement observed YBARRA conduct multiple transactions, which appeared to be withdrawals based upon law enforcement observing YBARRA retrieve what appeared to be currency at the conclusion of each transaction, while minor 1 stood alongside YBARRA. YBARRA appeared to conduct several withdrawal transactions in rapid succession while law enforcement observed for approximately nine minutes. YBARRA appeared to insert several different cards to conduct withdrawals, and put the retrieved cards in her pocket on multiple occasions. Based upon my training and experience, individuals conducting legitimate transactions at ATMs typically conduct a single transaction and do not transition between multiple payment cards rapidly to conduct several transactions in a short period of time.

40. USSS agents and Los Angeles District Attorney's Office investigators told me that while YBARRA was at the US Bank ATM, law enforcement learned from US Bank that the withdrawal transactions conducted by YBARRA took place on multiple EBT accounts, totaling approximately \$4,500.00.

41. A USSS analyst told me that law enforcement also learned from US Bank that YBARRA and minor 1 appeared on surveillance video at another US Bank ATM at 10990 Downey Avenue in Downey, California, just ten minutes before arriving at the US Bank ATM on Florence Avenue. According to US Bank data and surveillance video for the US Bank ATM on Downey Avenue, YBARRA attempted to withdraw \$840.00 in one transaction, which was declined due to insufficient funds, and successfully withdrew approximately \$3,260.00 in four separate transactions.

42. USSS agents and Los Angeles District Attorney's Office investigators told me that based on the date, time, ATM location, presence of multiple, and successive ATM withdrawals on multiple EBT cardholder accounts during a short time period, law enforcement identified YBARRA and minor 1 as EBT fraud suspects and watched as YBARRA and minor 1 returned to the SUBJECT VEHICLE. YBARRA was the driver of the SUBJECT VEHICLE and minor 1 was in the passenger seat of the SUBJECT VEHICLE as they began to exit the parking lot. Law enforcement initiated a traffic stop to detain YBARRA and minor 1. During the traffic stop of the SUBJECT VEHICLE, law enforcement identified an additional minor (hereafter, "minor 2") in the SUBJECT VEHICLE. Law enforcement learned that minor 2 is a sibling of minor 1.

43. USSS agents and Los Angeles District Attorney's Office investigators told me that law enforcement detained YBARRA, minor 1, and minor 2. Upon search incident to arrest of YBARRA, law enforcement located 17 gift cards containing sticky notes

with four-digit numbers. Based on my training and experience, I believe that the digits on the cards are PIN codes.

44. A USSS agent told me that YBARRA had approximately 17 cloned EBT cards on her person. One cloned EBT card was in YBARRA's back right pocket of her pants, and 16 cloned EBT cards were in YBARRA's front right pocket of her pants. The cloned cards consisted of a variety of re-encoded gift cards. The cards also had stickers placed on them with, what appeared to be, based on my training and experience, card balances and victim PINs.

45. A USSS analyst told me that law enforcement later determined through United States Department of Agriculture Office of Inspector General that the cards belonged to other individuals, not YBARRA. Moreover, the cloned cards also were affixed with stickers bearing victim PIN numbers that corresponded to each cloned card and were needed in order to conduct the unauthorized ATM withdrawals.

46. During an initial search of the SUBJECT VEHICLE, which I and another USSS agent conducted, we located four transaction receipts. Two of the receipts were receipts from School's First Credit Union. One of the receipts was for a balance inquiry that occurred on March 1, 2023, at approximately 06:00 a.m., and the other was for a \$2,000.00 transaction declined, which occurred on March 1, 2023, at approximately 06:00 a.m. Two of the other receipts were from Bank of the West. One of the receipts was for a declined transaction, which the receipt shows occurred on March 1, 2023, at approximately 07:39 a.m. The



other receipt was for a \$400.00 cash withdrawal, on March 1, 2023, at approximately 07:41 a.m.

47. During the search of the SUBJECT VEHICLE, which I and another USSS agent conducted, we located five additional gift cards with four-digit PINs written on stickers on the front of each card.

48. USSS agents told me that minor 2 also had approximately \$18,105.00 in cash in a pocket of her dress and approximately five cloned cards with PINs written on the front of the cards.

49. A USSS analyst told me that US Bank ATM surveillance photographs obtained by law enforcement also clearly depicted YBARRA at the ATM conducting the unauthorized withdrawals using numerous EBT cards and directly corroborated law enforcement's surveillance observations.

50. I retrieved the SUBJECT DEVICE from the SUBJECT VEHICLE on the center console during my search of the SUBJECT VEHICLE.

**V. TRAINING AND EXPERIENCE REGARDING IDENTITY THEFT CRIMES**

51. Based on my training and experience and information obtained from other law enforcement officers who investigate identity theft, I know the following:

a. It is common practice for individuals involved in identity theft, bank fraud, and access device fraud crimes to possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions and identity theft. Suspects often use

digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

b. Oftentimes identity thieves take pictures of items reflecting their stolen identities, including items retrieved from stolen mail or mail matter, with their cellphones.

c. It is also common for identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers. Identity thieves often keep such information in their cars, storage units, and in their digital devices.

d. It is common for identity thieves, and individuals engaged in bank fraud, access device fraud, and

identification document fraud to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. These types of devices are routinely kept where the person will have easy access to such devices, such as on their person or in their cars or homes or storage units. Software relevant to such schemes can also often be found on digital devices, such as computers.

e. Based on my training and experience, I know that individuals who participate in identity theft, bank fraud, and access device fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos. Suspects may also have paper copies of such records, which they may keep on their person or in their cars, homes, or storage units.

f. Individuals engaged in mail and identity theft often use multiple digital devices, which they may keep on their person or in their cars or homes.

**VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES<sup>1</sup>**

52. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

---

<sup>1</sup> As used herein, the term "digital device" includes the SUBJECT DEVICES as well as any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

53. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

54. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a

device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress YBARRA's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of YBARRA's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

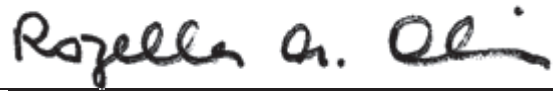
55. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

## **VII. CONCLUSION**

56. For all of the reasons described above, there is probable cause to believe that YBARRA has committed a violation of 18 U.S.C. § 1029(a)(2) (use of unauthorized access devices). There is also probable cause that the items to be seized described in Attachment B will be found in a search of the

SUBJECT DEVICE as described in Attachment A-1 and the SUBJECT  
VEHICLE as described in Attachment A-2.

Attested to by the applicant in  
accordance with the requirements  
of Fed. R. Crim. P. 4.1 by  
telephone on this 2nd day of  
March, 2023.

A handwritten signature in black ink, reading "Rozella A. Oliver". The signature is written in a cursive, flowing style. The first name "Rozella" is written in a larger, more prominent script, followed by "A." and "Oliver". The signature is positioned above a horizontal line.

THE HONORABLE ROZELLA A. OLIVER  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A-1**

PROPERTY TO BE SEARCHED

The following digital device (the "SUBJECT DEVICE"), seized on March 1, 2023 and currently maintained in the custody of the United States Secret Service in Los Angeles, CA: Samsung Galaxy A14 mobile device with IMEI 350545463176826.

**ATTACHMENT A-2**

PROPERTY TO BE SEARCHED

The following vehicle (the "SUBJECT VEHICLE"), impounded on March 1, 2023 and currently maintained in the custody of the Los Angeles Police Department in the County of Los Angeles: 2008 white Toyota Prius, bearing California license plate 8FCB613 and Vehicle Identification Number JTDEKB20U583455633 (the "SUBJECT VEHICLE").

**ATTACHMENT B**

**I. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information), 1029 (Fraud and Related Activity in Connection with Access Devices), 1344 (Bank Fraud), and 1028A (Aggravated Identity Theft), namely:

a. Access devices, access card skimming devices, and device-making equipment, including debit or credit cards, gift cards, or any other cards bearing magnetic stripes; equipment used for reading or making the same, such as skimming devices, card readers or magnetic stripe reading/encoding devices, embossers, tipplers, card printers, or the accessories required to use the same; electronic components for assembling and installing skimming devices; soldering mats or soldering residue; notes or logs of PIN numbers or ZIP codes;

b. Records, documents, or materials relating to cloned cards, including blank white plastic cards or debit, credit or gift cards that contains altered information on the card's magnetic stripe;

c. Records, documents, or materials relating to EBT cards, including, personal identification number (PIN), card holder's name, card holder's account number and card holder's expiration date;

d. Records, documents, or materials relating to ATM locations;

e. Cash or monetary instruments, including bundles of cash, as well as discrete stacks of cash totaling over \$1,000, including their packaging or wrapping, and any records tending to show the source of such cash; any amount of postal money orders, private money orders (i.e., "Money Gram" money orders), or casino chips or other negotiable or transferable instruments;

f. Data, records, documents, or information (including electronic mail and messages) pertaining to obtaining, possessing, using, or transferring personal and/or financial transaction identification information for persons other than Nevaeh Rosa YBARRA, such as names, addresses, phone numbers, credit and debit card numbers, security codes, bank account and other financial institution account numbers, Social Security numbers, email addresses, IP addresses, as well as PIN numbers and passwords for financial institutions or internet service providers;

g. Storage locations, including records indicating the location, ownership or control of any storage lockers, storage garages, trailers, residences, hotel rooms, rental premises, vaults, safe deposit boxes, or other locations where any digital devices, cash or monetary instruments, or access devices or device-making equipment may be stored, as well as any keys or access devices required to access the same;

h. Records, documents, or materials of who used, owned, or controlled the SUBJECT VEHICLE or the SUBJECT DEVICES at the time the things described in this warrant occurred;

i. Records, documents, programs, applications, or materials pertaining to applications for, or use of, credit or debit cards, bank accounts, or merchant processor accounts;

j. Data, records, documents (including e-mails), or information reflecting or referencing purchases of merchandise, securities, electronic currency, and other valuable things;

k. Software, devices, or tools used to obtain, create, or use counterfeit or unauthorized checks, coupons, or access devices such as credit, debit, bank, and gift cards;

l. Any documents or records relating to any bank accounts, credit card accounts, or other financial accounts;

m. Records, documents, programs, applications, or materials relating to United States mail or mail matter;

n. Contents of any calendar or date book stored on any of the digital devices;

o. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

p. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show address book information, including all stored or saved telephone numbers;

q. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to

show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

r. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

s. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

t. Audio recordings, pictures, video recordings, or still captured images of United States mail or mail matter, whether opened or unopened, or relating to the possession or distribution of drugs or the collection or transfer of the proceeds of the above-described offenses; and

u. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof, including but not limited to the SUBJECT DEVICES.

v. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

vii. records of or information about Internet Protocol addresses used by the device.

2. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in

digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

## **II. SEARCH PROCEDURE FOR DIGITAL DEVICES**

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall



complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. During the execution of this search warrant, law enforcement is permitted to: (1) depress Nevaeh Rosa YBARRA's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of Nevaeh Rosa YBARRA's face with her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not

apply to any search of digital devices pursuant to any other court order.